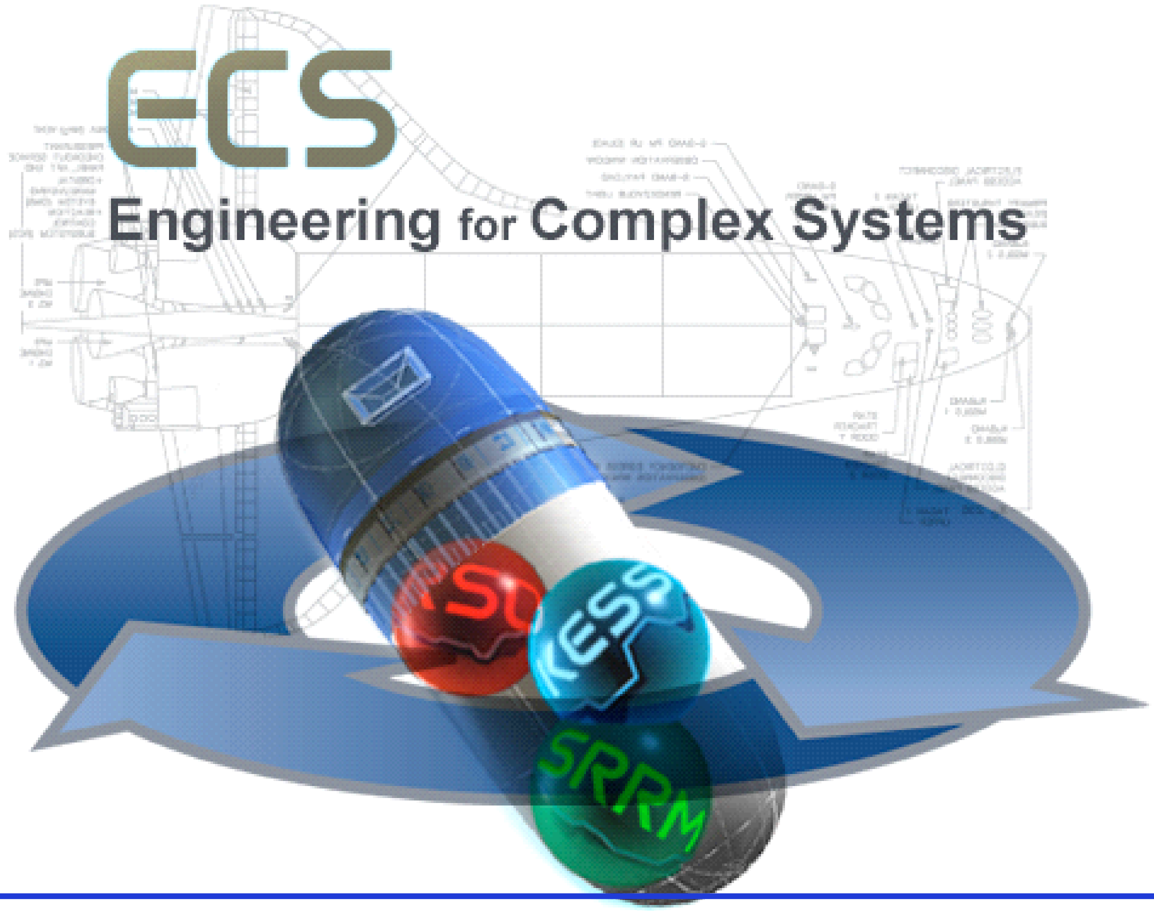
Risk & Safety in Complex Systems
Panel #6

The nature of acceptable risk and NASA's commitment to safety is a topic that touches all of NASA's programs, and is relevant to any large technology effort, whether public or private. This panel will explore the elements that should go into a technologically-enabled advanced risk management framework for NASA that provides end-to-end capabilities.

Moderator: Yuri Gawdiak

Panel Members
- Howard McCurdy, American University
- Mark Shirley, Ames Research Center
- Michael Evangelist, Carnegie Mellon University
- James Williams, Sverdrup



Risk & Safety in Complex Systems

June 11, 2003

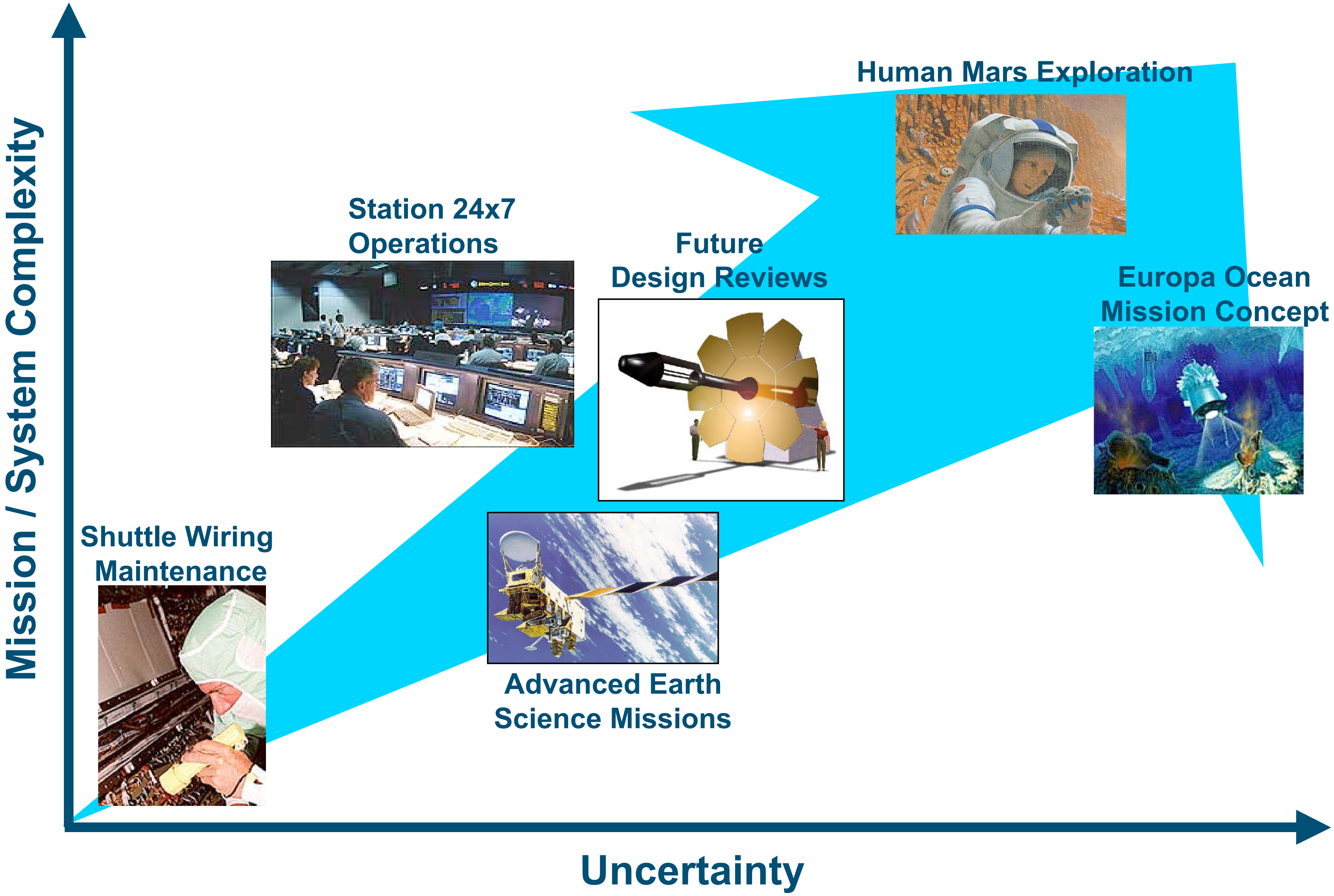
Turning Goals into Reality Conference

NASA's Vision - To improve life here

The ECS Initiative was generated in response to failures & shortfalls in our ability to develop and management complex systems

Current & Future Challenges & Risks

"…To extend life to there, To find life beyond."



Mission / System Complexity

Uncertainty

Shuttle Wiring Maintenance

Station 24x7 Operations

Advanced Earth Science Missions

Future Design Reviews

Human Mars Exploration

Europa Ocean Mission Concept

The NASA Vision

To improve life here,
To extend life to there,
To find life beyond.

The NASA Mission

To understand and protect our home planet,
To explore the universe and search for life,
To inspire the next generation of explorers
... as only NASA can.

Program Formulation Study

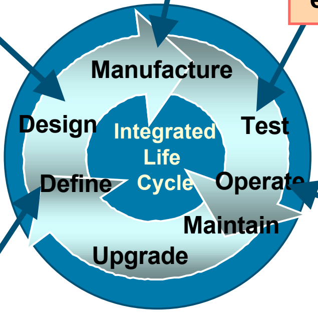
Case Studies: Mars Polar Lander

Sensors in the lander's legs send false positive signals upon leg deployment. The control software incorrectly retains the initial sensor signals and terminates engine thrust when control is enabled at 40 meters altitude. The lander accelerates and crashes into the planet surface.

Mis-wiring of test article prevents total system, full mission testing

Software validation and verification is insufficient to identify initialization error

Sensor-leg deployment interaction and consequences not understood.



On-board control system does not over-ride engine shut-down although contradictory evidence is available

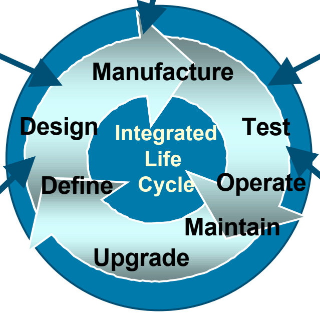
Project organization precludes adequate communication and oversight

Significant problems

Hardware condition is assured using automated inspection methods and intelligent signal processing

Software implementation is assured through automated testing and testability analyses

Risk advisor identifies criticality of sensors and alerts designers to mitigation requirements.



Organization modeling identifies risk to project success and corrective action

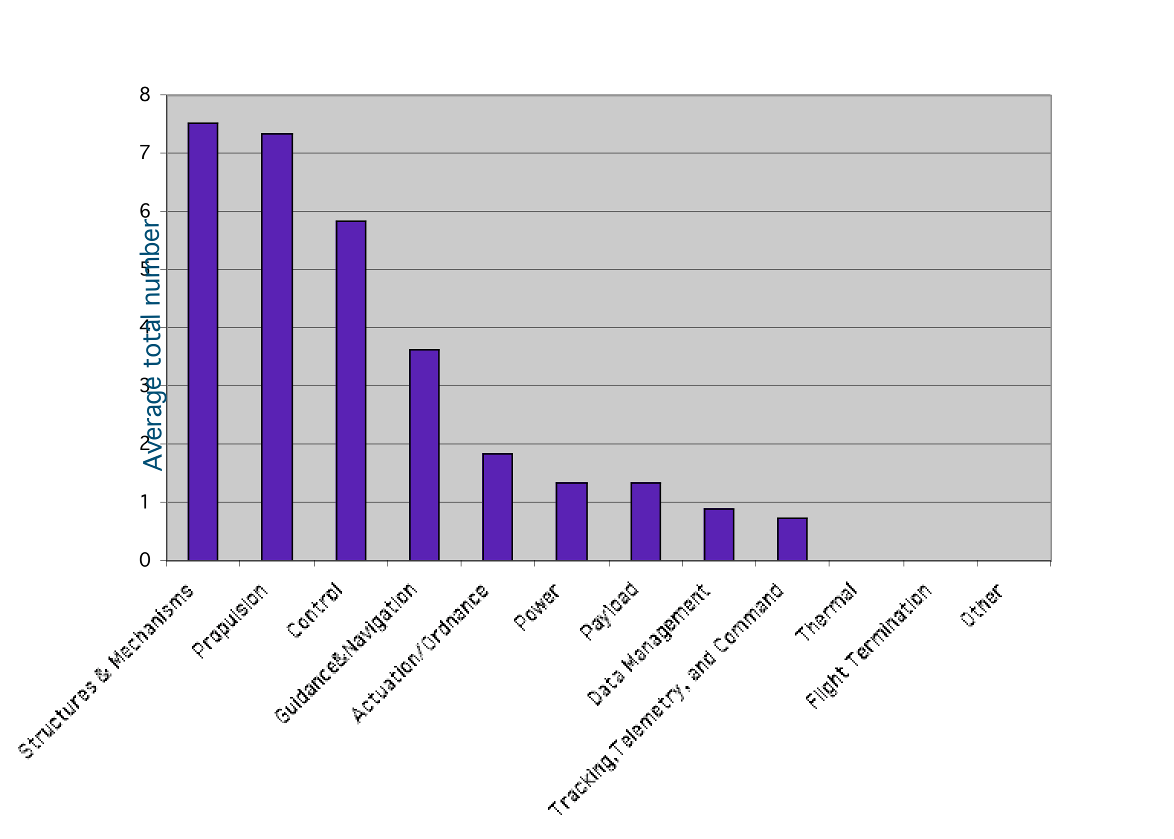
State-identification based controller uses available information to determine that touchdown could not have occurred yet and maintains engine thrust

Problem Specific Solutions

Program Formulation Study

MCC: Preliminary Data

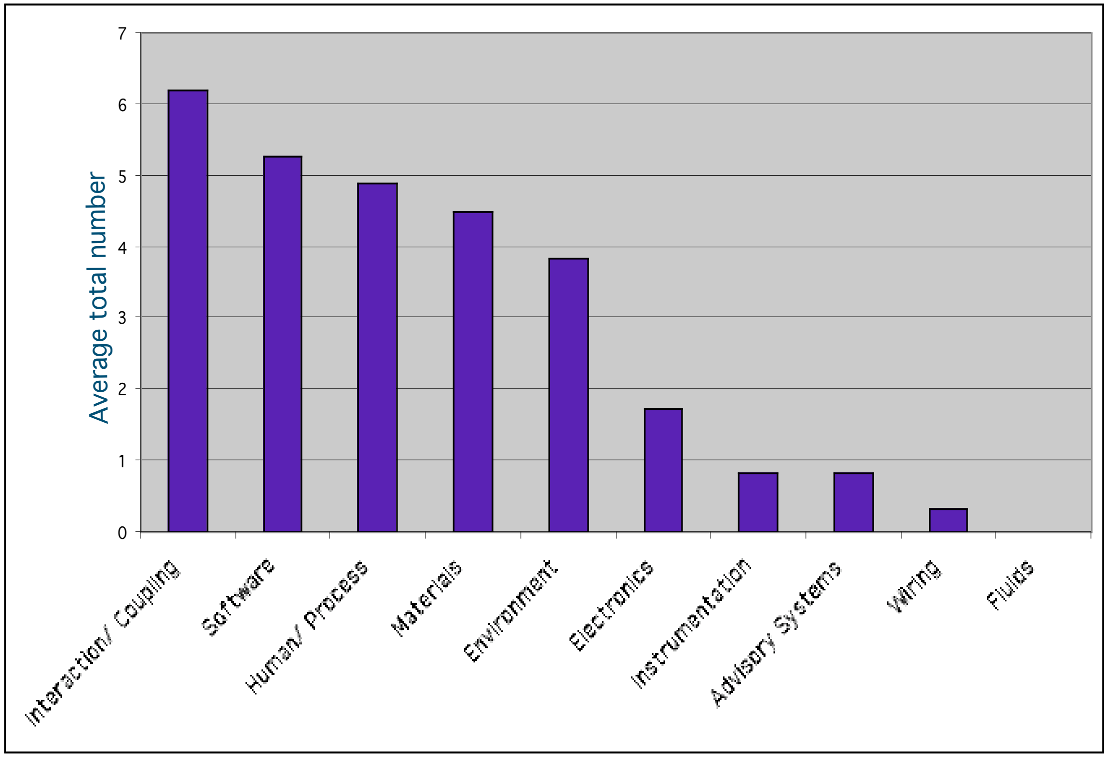
- Subsystems most often involved in mishaps:
  - Structures & mechanisms
  - Propulsion
  - Control
  - Guidance and navigation



Program Formulation Study

MCC: Preliminary Data

- Most frequent cross-system elements involved in mishaps:
  - Subsystem interactions
  - Software
  - Humans-in-the–loop processes
  - Materials
  - Environment

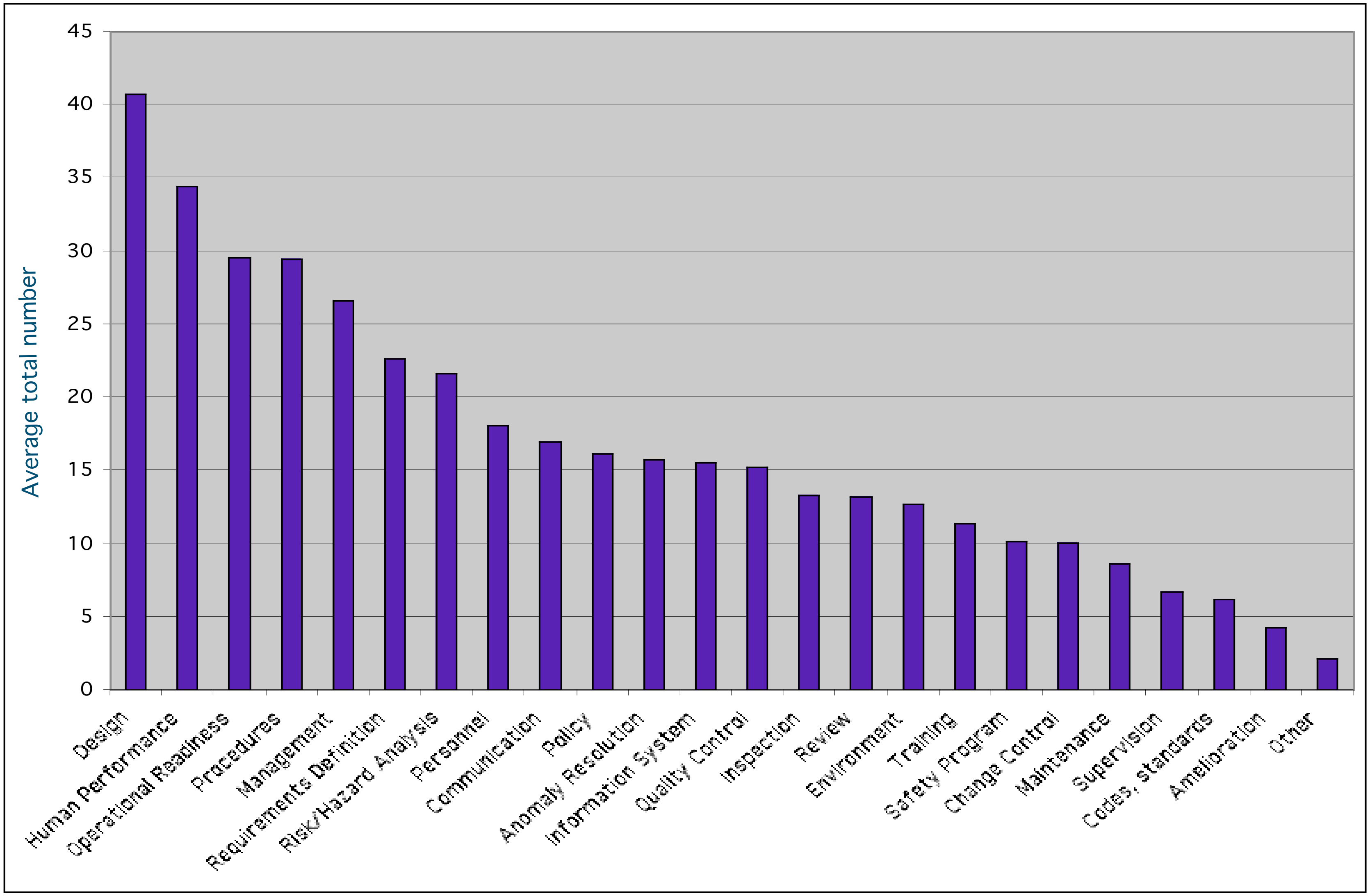


Program Formulation Study

MCC: Preliminary Data

Most frequently cited categories of 21 mishaps studied:

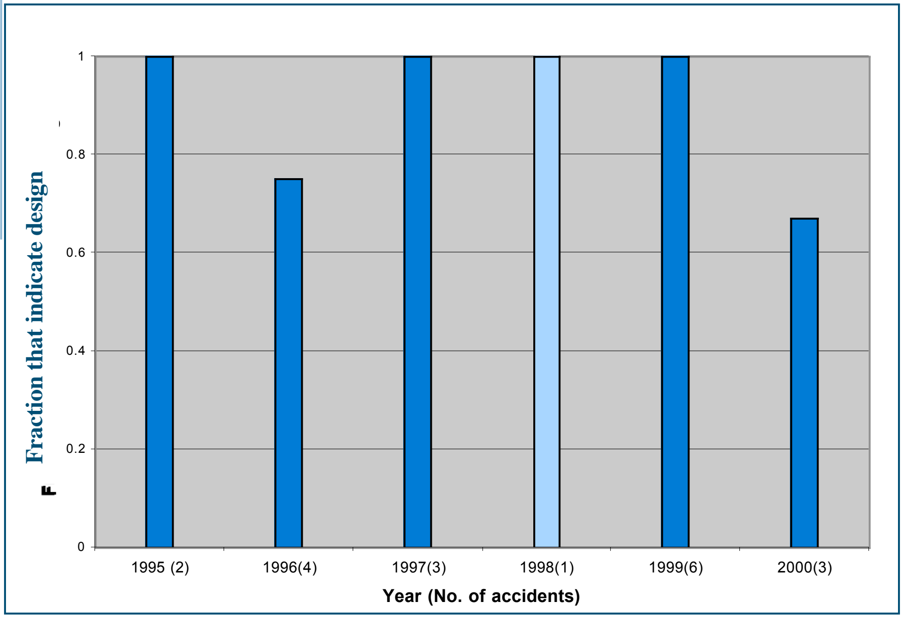
- insufficiencies in design, test, and management processes
- limitations of human performance and procedure implementation

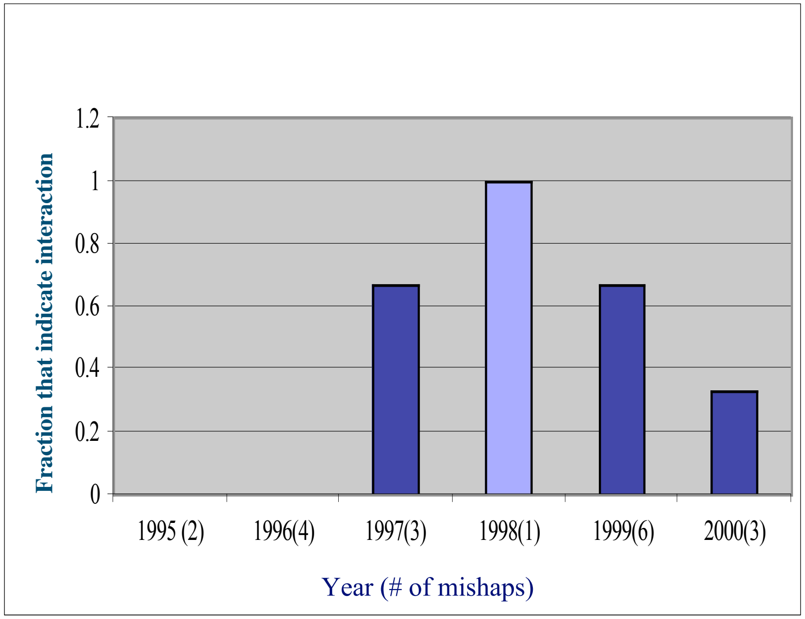


Program Formulation Study

MCC: Example Trends

Initial trends garnered from 21 mishaps suggest:



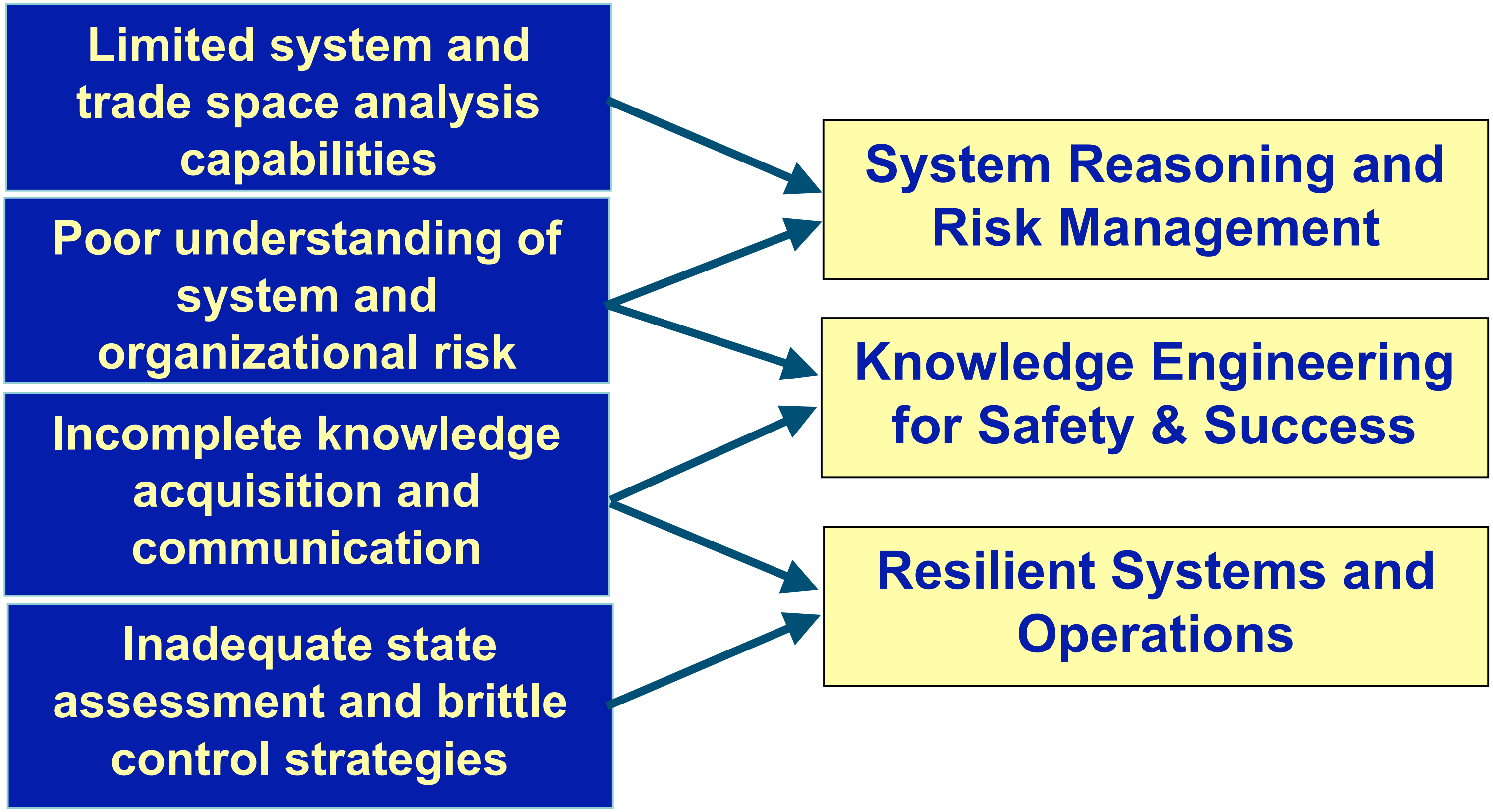


Design problems remain consistently high since 1995

Unintentional subsystem interactions become significant after 1997

Program Formulation Study

Revised Problem Classes



Limited system and trade space analysis capabilities

Poor understanding of system and organizational risk

Incomplete knowledge acquisition and communication

Inadequate state assessment and brittle control strategies

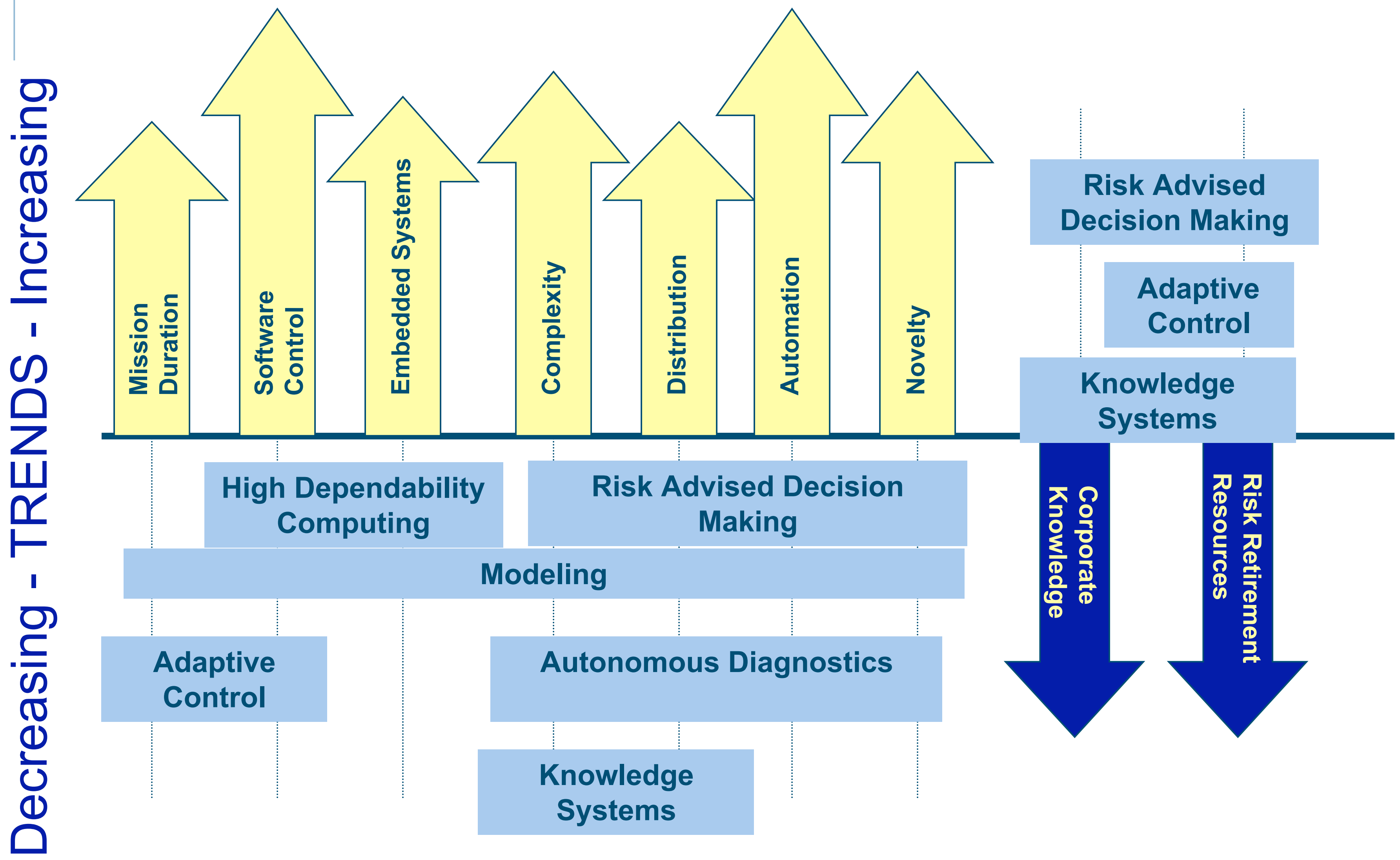
System Reasoning and Risk Management

Knowledge Engineering for Safety & Success

Resilient Systems and Operations

Program Formulation Study

Solution Class to Trend Class Mapping



Decreasing - TRENDS - Increasing

Mission Duration

Software Control

Embedded Systems

Complexity

Distribution

Automation

Novelty

Risk Advised Decision Making

Adaptive Control

Knowledge Systems

Corporate Knowledge

Risk Retirement Resources

High Dependability Computing

Risk Advised Decision Making

Modeling

Adaptive Control

Autonomous Diagnostics

Knowledge Systems

Program Overview

ECS Executive Overview

Objectives

- Develop tools and technologies to understand and reduce agency-wide mission risks
- Help develop and test the feasibility of resiliency technologies for human-rated systems
- Motivate & enhance student education through demonstrations & applications of ECS unique technologies & research

Requirements

- Address limited system & trade space analysis capabilities
- Address poor understanding of system, human, and organizational risk
- Address incomplete knowledge acquisition and communication
- Address inadequate state assessment and brittle control strategies

Challenges

- System risk and uncertainties not well represented, understood nor managed
- Human, Organization & Cultural limitations in perceiving & managing risks
- Volume of data and interactions in complex systems are difficult to manage
- Expanding use of software limits ability to decipher all end-states
- Increasingly difficult mission environments & objectives

Approach

- Risk-based Decision Support
- Model Based Reasoning
- Human & Organizational Modeling
- Integrated Knowledge Management Tools
- Resilient & Adaptive System Architectures
- Advanced Software Engineering Tools

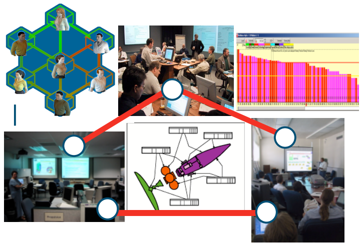
Products

- Risk Tool Suite for Advanced Design
- Investigation Methods & Tools
- Virtual Iron Bird Technologies
- Organizational Risk Technologies
- Resilient System Technologies
- Software Dependability Metrics & Tools

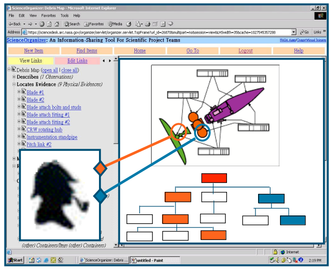
Program Overview

ECS Program Product Classes

System Reasoning & Risk Management



Risk Tool Suite for Advanced Design



ScienceOrganizer: Debris Map - Microsoft Internet Explorer

Address https://sciencedesk.arc.nasa.gov/organizer/servlet/organizer.servlet.TopFrame?url_id=268708multipart=no&session=view&LHSwidth=358cache=1027545357288

ScienceOrganizer: An Information-Sharing Tool For Scientific Project Teams

NASA Ames/Computational Sciences

Debris Map (open all | close all)

Describes (1 Observations)

Locates Evidence (9 Physical Evidences)

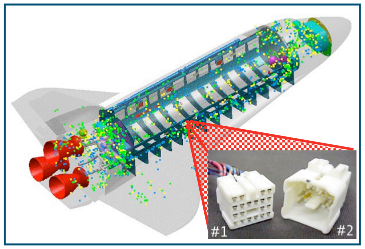
- Blade #1
- Blade #2
- Blade attach bolts and studs
- Blade attach fitting #1
- Blade attach fitting #2
- CRW rotating hub
- Instrumentation standpipe
- Pitch link #2

(other) Containers/Item (other) Containers)

Investigation Methods and Tools

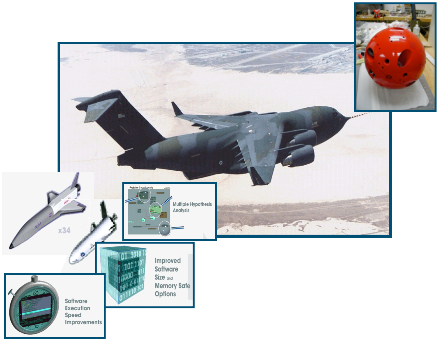
Knowledge Engineering for Safety & Success

Organization Risk Technologies



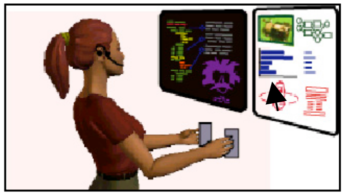
Virtual Iron Bird Technologies

Resilient Systems & Operations



x34
Multiple Hypothesis Analysis
Improved Software Size and Memory Safe Options
Software Execution Speed Improvements

Resilient System Technologies



Software Dependability Metrics & Tools

BACKUP CHARTS

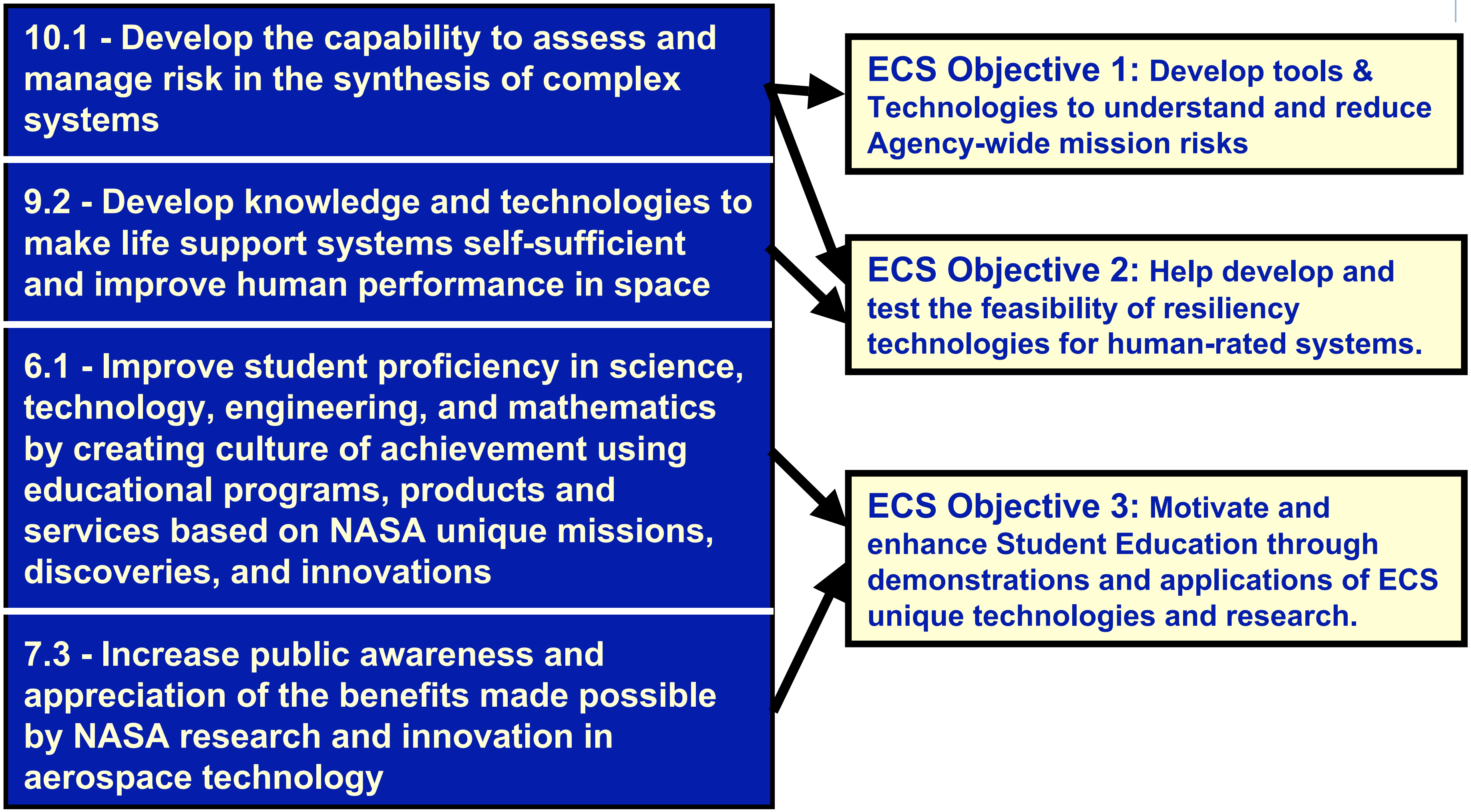
Program Overview

Program Objectives Flow

ECS Theme Objectives

(in highest to lowest priority order)

ECS Program Objectives



10.1 - Develop the capability to assess and manage risk in the synthesis of complex systems

9.2 - Develop knowledge and technologies to make life support systems self-sufficient and improve human performance in space

6.1 - Improve student proficiency in science, technology, engineering, and mathematics by creating culture of achievement using educational programs, products and services based on NASA unique missions, discoveries, and innovations

7.3 - Increase public awareness and appreciation of the benefits made possible by NASA research and innovation in aerospace technology

ECS Objective 1: Develop tools & Technologies to understand and reduce Agency-wide mission risks

ECS Objective 2: Help develop and test the feasibility of resiliency technologies for human-rated systems.

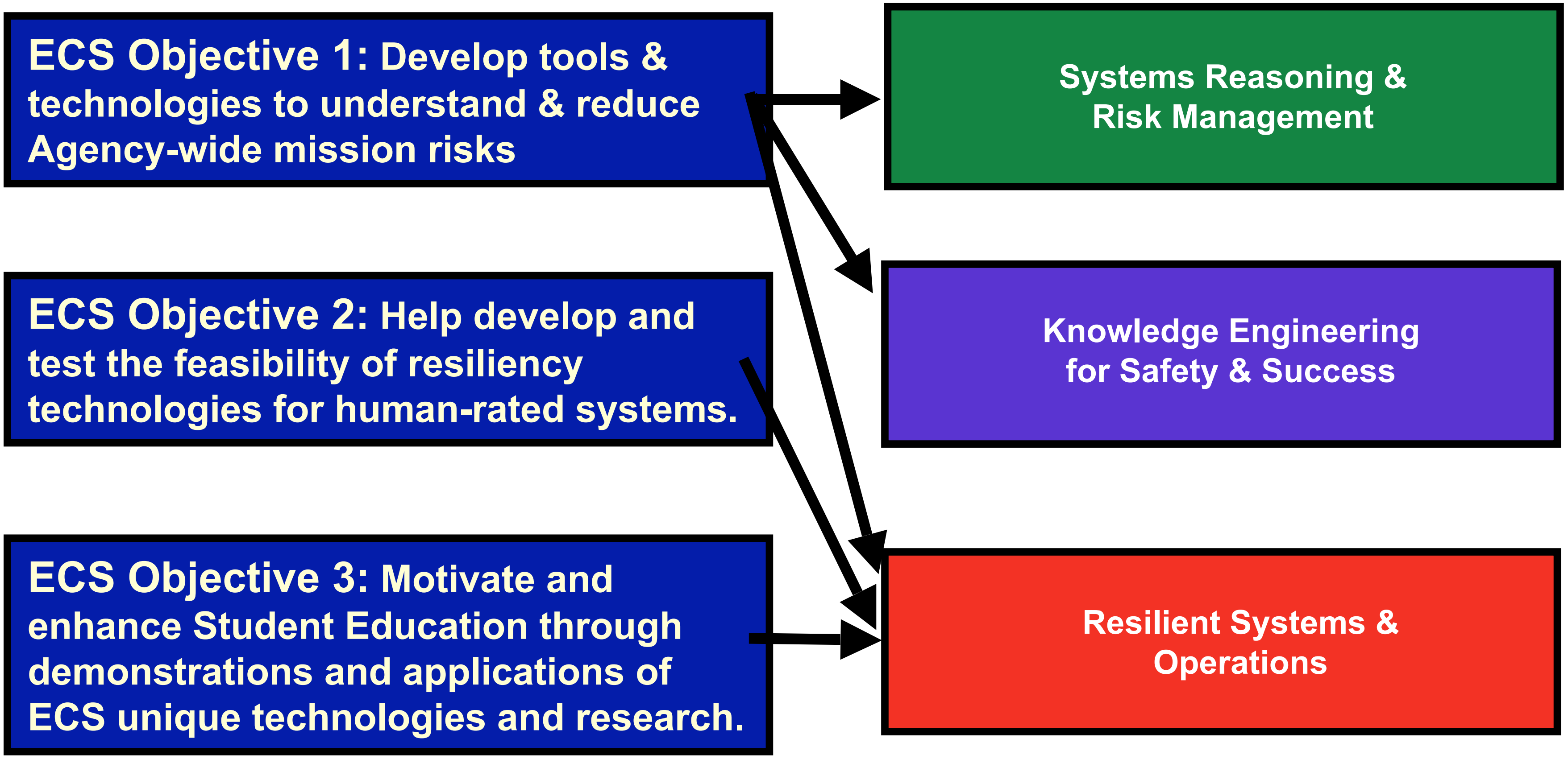
ECS Objective 3: Motivate and enhance Student Education through demonstrations and applications of ECS unique technologies and research.

Program Overview

Program Objectives Flow (cont.)

ECS Program Objectives

ECS Projects



ECS Objective 1: Develop tools & technologies to understand & reduce Agency-wide mission risks

ECS Objective 2: Help develop and test the feasibility of resiliency technologies for human-rated systems.

ECS Objective 3: Motivate and enhance Student Education through demonstrations and applications of ECS unique technologies and research.

Systems Reasoning & Risk Management

Knowledge Engineering for Safety & Success

Resilient Systems & Operations

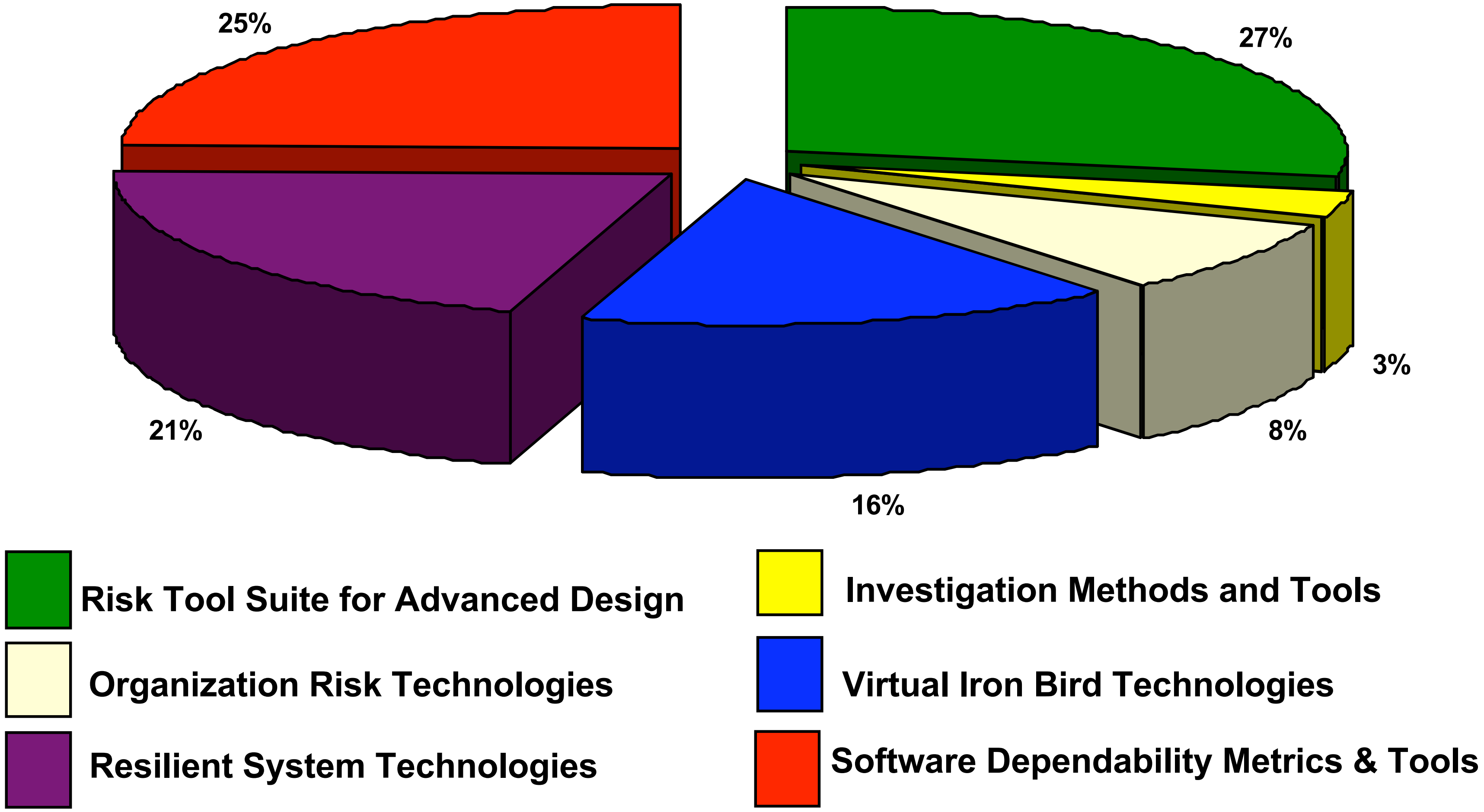
Program Overview

Program Budget

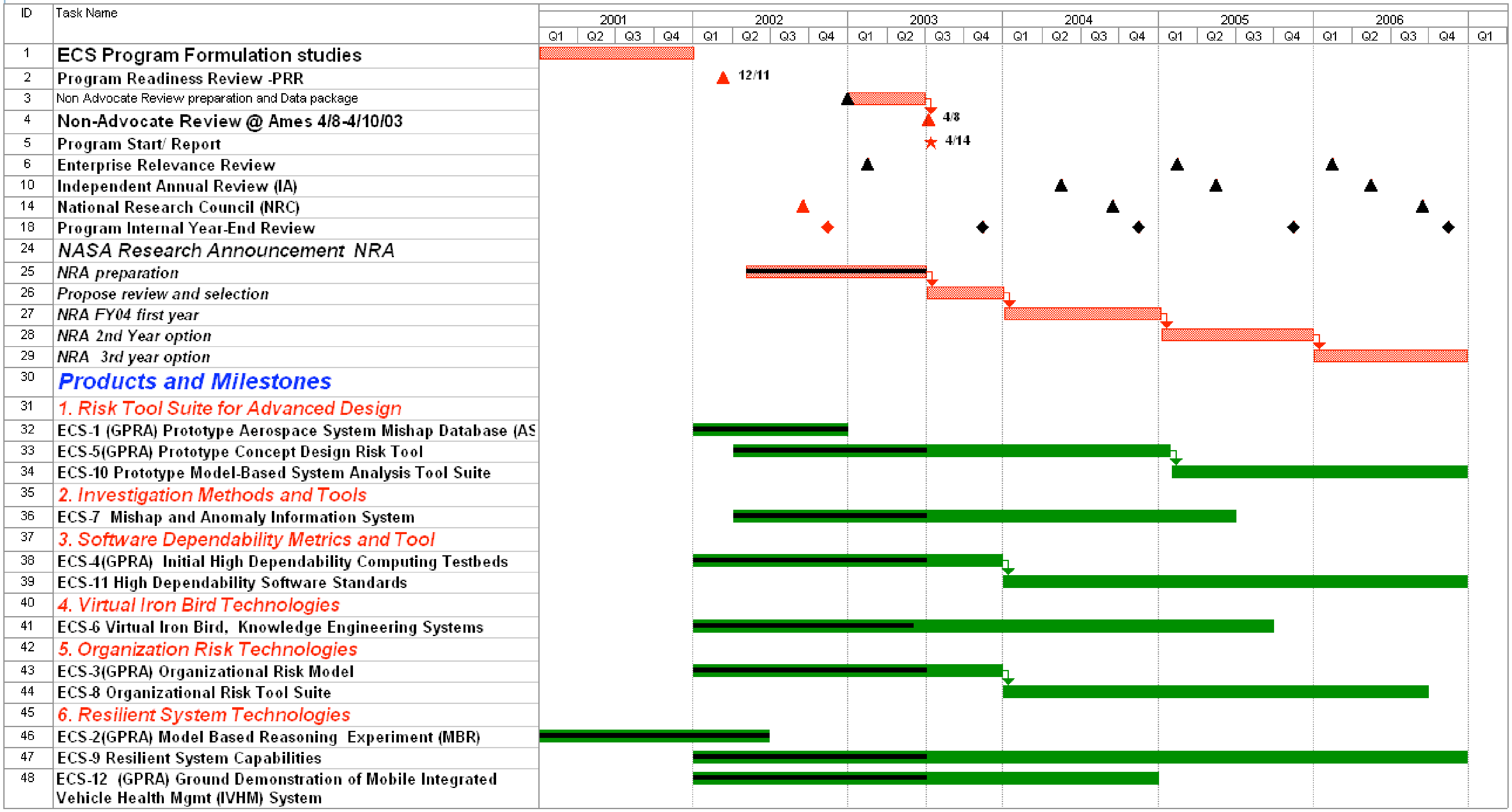
Engineering for Complex Systems	FY02	FY03	FY04	FY05	FY06	Total
0.0 Headquarters Assessment	1.400	1.400	1.370	1.375	1.375	6.920
1.0 Program Office						
1.01 Program Management	3.015	2.875	1.811	1.744	1.944	11.398
1.02 NASA Research Announcement	0	0.238	0.425	0.425	.425	1.513
1.03 Education Outreach	0.150	0.149	0.200	0.150	0.150	0.799
2.0 System Reasoning and Risk Management						
2.0.1 Project Management	0.174	0.298	0.300	0.300	0.300	1.372
2.0.2 NASA Research Announcement	0	0	1.000	1.000	1.000	3.000
2.0.4 Risk Methods / Tools Verification & Validation	0.175	0.174	0.225	0.600	1.000	2.174
2.1 Risk Tool Suite	2.027	1.946	1.800	1.700	1.700	9.173
2.2 Core Risk Research	3.887	3.630	3.261	3.214	3.550	17.542
2.3 Investigation Methods & Tools	0.325	0.667	0.700	0.650	0.700	3.042
3.0 Knowledge Engineering for Safety & Success						
3.0.2 NASA Research Announcement	0	0	0.850	0.800	0.850	2.500
3.1 Human & Organizational Risk Management	1.798	1.637	1.600	1.600	2.450	9.085
3.2 Engineering Information Management	3.138	3.257	2.872	3.122	3.095	15.484
4.0 Resilient Systems & Operations						
4.0.1 Formulation Project Management	0.099					0.099
4.0.3 NASA Research Announcement	0	0	0.150	0.200	0.200	0.550
4.1 Intelligent & Adaptive Operations and Control	6.079	5.603	4.330	4.208	4.174	24.394
4.2 Resilient Software Engineering	5.733	5.544	6.506	6.412	4.587	28.782
Total	**28.000**	**27.418**	**27.400**	**27.500**	**27.500**	**137.827**

Program Overview

Program Budget Allocation to Products



Program Overview
Program Schedule



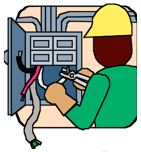
ID	Task Name
1	ECS Program Formulation studies
2	Program Readiness Review -PRR
3	Non Advocate Review preparation and Data package
4	Non-Advocate Review @ Ames 4/8-4/10/03
5	Program Start/ Report
6	Enterprise Relevance Review
10	Independent Annual Review (IA)
14	National Research Council (NRC)
18	Program Internal Year-End Review
24	*NASA Research Announcement NRA*
25	*NRA preparation*
26	*Propose review and selection*
27	*NRA FY04 first year*
28	*NRA 2nd Year option*
29	*NRA 3rd year option*
30	***Products and Milestones***
31	*1. Risk Tool Suite for Advanced Design*
32	ECS-1 (GPRA) Prototype Aerospace System Mishap Database (AS
33	ECS-5(GPRA) Prototype Concept Design Risk Tool
34	ECS-10 Prototype Model-Based System Analysis Tool Suite
35	*2. Investigation Methods and Tools*
36	ECS-7 Mishap and Anomaly Information System
37	*3. Software Dependability Metrics and Tool*
38	ECS-4(GPRA) Initial High Dependability Computing Testbeds
39	ECS-11 High Dependability Software Standards
40	*4. Virtual Iron Bird Technologies*
41	ECS-6 Virtual Iron Bird, Knowledge Engineering Systems
42	*5. Organization Risk Technologies*
43	ECS-3(GPRA) Organizational Risk Model
44	ECS-8 Organizational Risk Tool Suite
45	*6. Resilient System Technologies*
46	ECS-2(GPRA) Model Based Reasoning Experiment (MBR)
47	ECS-9 Resilient System Capabilities
48	ECS-12 (GPRA) Ground Demonstration of Mobile Integrated Vehicle Health Mgmt (IVHM) System

Program Formulation Study

Mishap Sub-causes

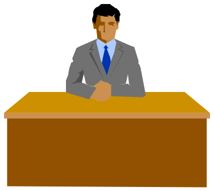
Design

- Misunderstanding system attributes, behavior
- Errors and omissions
- Operational constraints missed



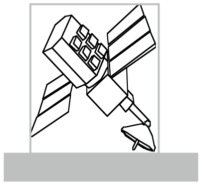
Procedures

- No procedures or not followed
- Ambiguous directions
- Insufficient to control, prevent



Management

- Flawed decision-making practices
- Organization structure issues
- Problems, issues not visible
- Resource pressures



Operational Readiness

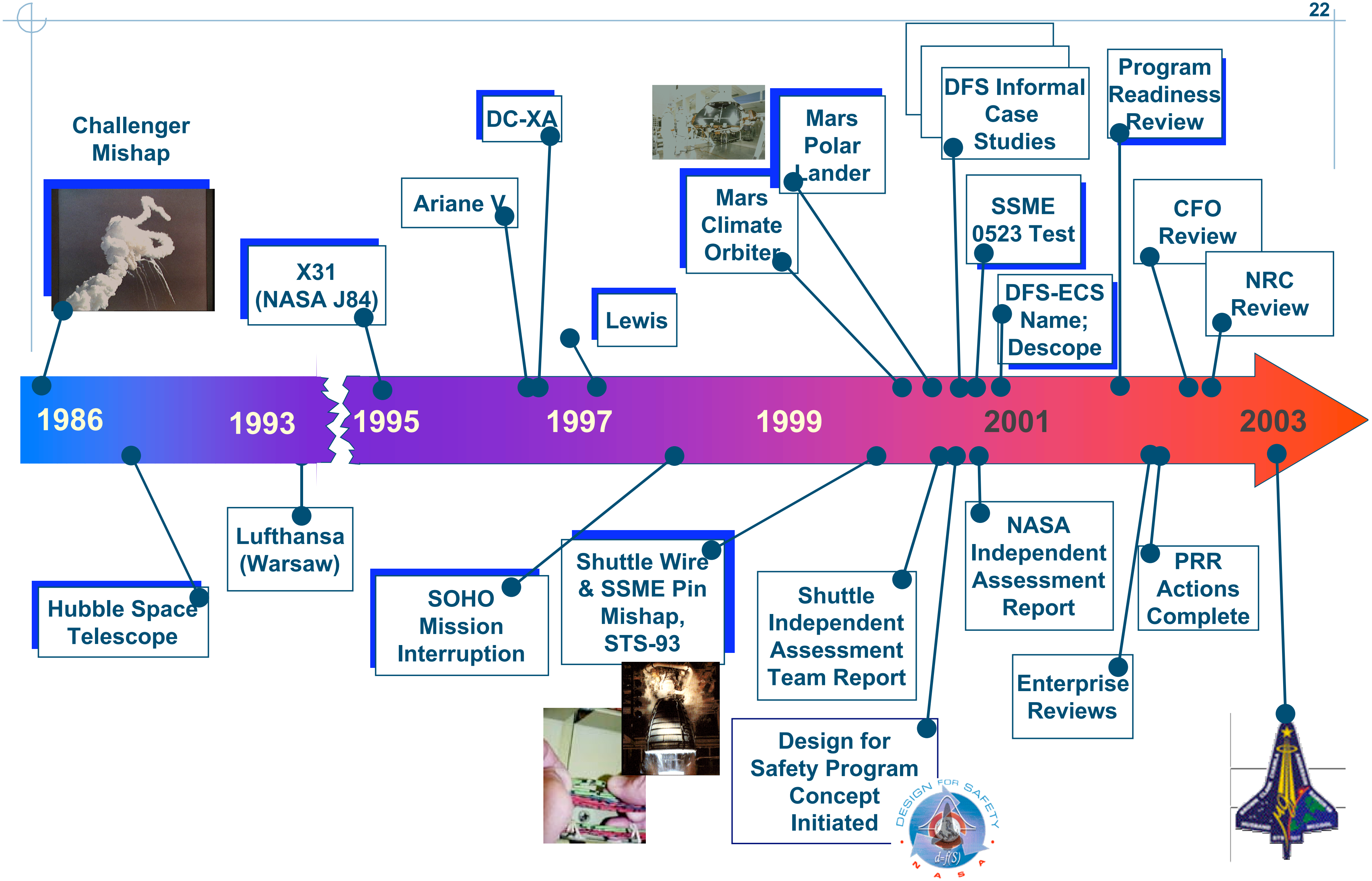
- Misunderstanding test data
- Tests, system not representative
- Inadequate sensing

Human Performance

- Cognitive problems (reasoning, understanding)
- Omission, errors
- Communication
- Human factors issues (e.g. work environment)

Program Background

Formulation Timeline



1986
1993
1995
1997
1999
2001
2003
Challenger Mishap
Hubble Space Telescope
Lufthansa (Warsaw)
X31 (NASA J84)
Ariane V
DC-XA
SOHO Mission Interruption
Lewis
Mars Climate Orbiter
Mars Polar Lander
Shuttle Wire & SSME Pin Mishap, STS-93
Shuttle Independent Assessment Team Report
DFS Informal Case Studies
Design for Safety Program Concept Initiated
SSME 0523 Test
NASA Independent Assessment Report
DFS-ECS Name; Descope
Program Readiness Review
Enterprise Reviews
CFO Review
PRR Actions Complete
NRC Review
DESIGN FOR SAFETY
d=f(S)
NASA